



INSTALLATION AND OPERATION MANUAL



INDUSTRIALLY HARDENED HIGH PERFORMANCE
WIRELESS ETHERNET

**This manual serves the following
ComNet Series:**

NW1
NW9
NW1/M

Thank you for purchasing NetWave® from ComNet. This installation guide applies to all NetWaveRadios.

The NetWave industrially hardened wireless Ethernet transmission link from ComNet can be configured through the embedded User Interface as an AccessPoint. This point-to-multipoint model allows multiple Ethernet endpoints to be connected to a central AccessPoint. NetWave Radios support up to 500Mbps with their fastest radio using MIMO Technology. An easy to read LED array displays unit operational status along with received signal strength ensuring optimal installation and operation. The NW1, NW9 and NW1/M family of radios all support 802.3af

FCC radios are certified for the United States. IC radios are certified for Canada.

About This Guide

This guide is intended for different users such as engineers, integrators, developers, IT managers, and technicians.

It assumes that users have some PC competence and are familiar with Microsoft Windows operating systems and web browsers such as Windows Internet Explorer and Mozilla Firefox, as well as have knowledge of the following:

- » Installation of electronic equipment
- » Electrical regulations and guidelines
- » Knowledge of Local Area Network technology

Related Documentation

The following documentation is also available:

- » NW1 Datasheet
- » NW9 Datasheet
- » NW1/M Datasheet
- » NetWave Quick Start Guide

Website

For information on ComNet's entire product line, please visit the ComNet website at <http://www.comnet.net>

Support

For any questions or technical assistance, please contact your sales person (sales@comnet.net) or the customer service support center (techsupport@comnet.net)

Safety

- » Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.
- » The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority.

Contents

About This Guide	2
Overview	5
Legal Information	5
1.0 Introduction	6
1.1 System Requirements	6
2.0 Cabling Requirements	7
3.0 Hardware Installation	7
Outdoor Ethernet Gland Installation	
NetWave Indicating LED Details	9
Outdoor Standard Mounting Hardware	9
4.0 Key Default Configurations	10
5.0 Quick Configuration	11
6.0 Detailed Configuration	12
Getting Started	12
Buttons and Alerts	13
7.0 Status Tab	14
Overview	14
Wireless AP	15
Associated Stations AP	16
System	17
Memory	17
Network	17
DHCP Leases	17
Routes	18
System Log	18
Kernel Log	19
Real-time Graphs	20

8.0 System Tab	23
System Properties	23
General Settings	23
Logging	24
Language and Style	24
SSH	25
Services	26
Auto Reboot	29
WiFi –Overview	30
WiFi – Wireless Network	32
9.0 Network Tab	36

Overview

Legal Information

No part of this document may be reproduced or transmitted in any form or by any means, electronic and mechanical, for any purpose, without the express written permission of ComNet.

Copyright

Copyright © 2015 Communication Networks, LLC (dba ComNet). All rights reserved.

Disclaimer

ComNet reserves the right to make changes in specifications at any time without notice. The information furnished by ComNet in this material is believed to be accurate and reliable. However, ComNet assumes no responsibility for its use.

1.0 Introduction

The NetWave industrially hardened wireless Ethernet transmission link from ComNet can be configured through the embedded User Interface as an Access Point. This point-to-multipoint model allows multiple Ethernet endpoints to be connected to a central Access Point.

NetWave Radios support up to 500Mbps with their fastest radio using MIMO Technology. An easy to read LED array displays unit operational status along with received signal strength ensuring optimal installation and operation. The NW1, NW9 and NW1/M family of radios support 802.3af .

This user manual is a guide for the NetWave Wireless Radios as well as the preconfigured kits. ComNet NetWave Wireless offers OpenWRT with the most advanced Qualcomm Atheros wireless drivers. NetWave now includes a new user-friendly LuCI web interface for configuring the device. OpenWRT is an extensible GNU/Linux distribution for embedded devices. It is built from the ground up to be a full-featured, easily modifiable operating system. It is powered by a Linux kernel that's more recent than most other distributions. LuCI is a free, clean, extensible and easily maintainable web user interface for embedded devices. It has high performance, small installation size, fast runtimes, and good maintainability. The units come configured point to multipoint applications.

This manual contains detailed operational and configuration information not covered in the quick start guides. There some variations in features with each model, please consult the appropriate data sheet for features and capabilities.

This guide applies toall NetWave Radios.

1.1 System Requirements

Operating System:

Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Linux, or Mac OS X.

Web Browser:

Mozilla Firefox, Google Chrome, Apple Safari, or Microsoft Internet Explorer 8 or above.

2.0 Cabling Requirements

Shielded CAT 5 or better should be used for all out of plant Ethernet connection and should be properly grounded through the PoE AC ground. Industrial grade shielded Ethernet cable is recommended to help prevent ESD damage commonly experienced with outdoor installations. Visit www.comnet.net/comnet-products/cables

3.0 Hardware Installation

Outdoor Ethernet Gland Installation

There will be at least one cable gland included with each outdoor enclosure. Below is an image of the individual parts of the gland with an Ethernet cable routed through.

Note: The split rubber washer allows a pre-terminated Ethernet cable to be used. Use RJ-45 connector without Snagless Jacket.

Once the cable has been routed through the weather connection, and the RJ45 connection has been made, screw in the gland into the housing making sure it is tight enough for a water tight seal. Push the split rubber gasket into place and loosely screw the cap that goes over the rubber washer.



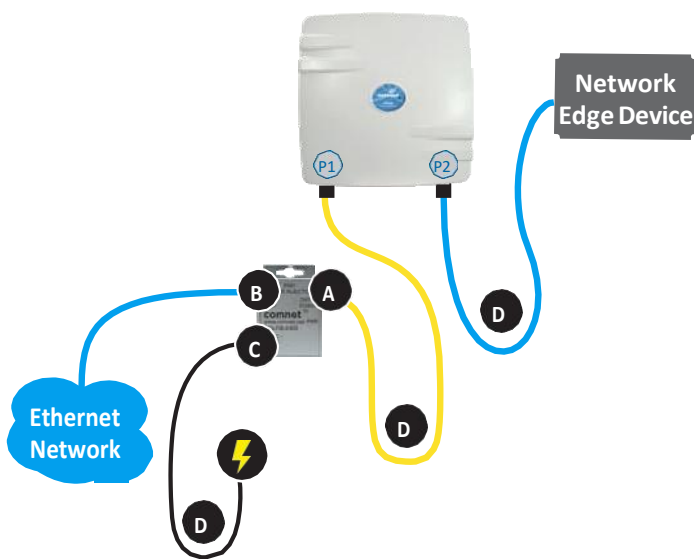
Once the gland is tight in the housing, tighten the outer nut/cap making sure the rubber seal squeezes and seals the Ethernet cable to the gland as shown below.

Connect one end of an RJ-45 Ethernet cable to the LAN OUT port of the Power Injection Module (PIM) and the other end to LAN of the access point – as shown below.

Note: Maximum length of the RJ-45 CAT5 cable is 90 meters.

Connect the RJ-45 Ethernet cable attached to the PIM to a network device, such as a switch or to the configuration PC. Then plug the power adaptor to an AC power outlet and power plug into the socket of the PIM – as shown in the diagram below.

Note: DC Passive PoE input for the NetWave Radios is 24 - 48VDC.

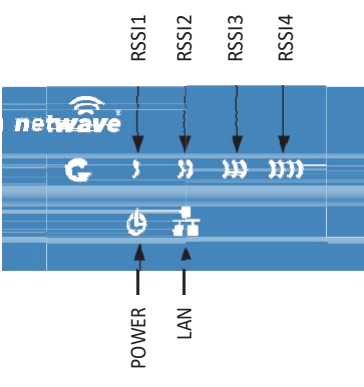


- A. Connect one end of an RJ-45 Ethernet cable to the OUT port of the Power Injection Module (PIM) and the other end to LAN of the access point. Maximum length of the RJ-45 CAT5 cable is 100 meters.*
- B. Connect the RJ-45 Ethernet cable attached to the PIM to a network device, such as a switch or to the PC you will use to configure the access point.
- C. Connect the power adaptor to the main electrical supply and the power plug into the socket of the PIM.
- D. A Drip Loop is recommended as additional precaution against moisture entering the Access Point housing.

**Up to 200mW radio. For higher power radio upgrade to higher rating power adapter.*

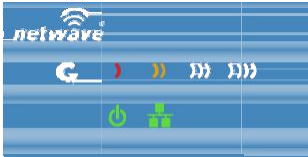
IMPORTANT: Only plug PoE power to Port 1.
Connecting a PoE power source to the PSE Port(#2) will cause a major device malfunction and void the warranty.

NetWave Indicating LED Details



LED	VISUAL CUE	INDICATION
POWER	SOLID GREEN	Power is supplied to the unit
	OFF	No power is supplied to the unit or the unit is in reset.
LAN	SOLID GREEN	LAN Connected
	OFF	No Connectivity
RSSI1	SOLID RED	Weak Connection
RSSI2	SOLID ORANGE	Moderate Connection
RSSI3	SOLID GREEN	Solid Connection
RSSI4	SOLID GREEN	Excellent Connection (Advisable to check Status Page to confirm RSSI is > -55)

SIGNAL STRENGTH:



WEAK SIGNAL

EXCELLENT SIGNAL

Outdoor Standard Mounting Hardware

This mounting hardware will support pole diameters up to 2 in (5.8 cm). Below are the parts contained in the standard mounting hardware.



Here is the mounting hardware assembled shown with a NW1/M in a +30° and -30°vertical position



4.0 Key Default Configurations

IP Address of Web Server	192.168.10.100 192.168.10.101 for all others
LAN Mode for Web Server	Static Addressing
Web Server User ID	admin
Web Server Password	admin
SSID	NetWave-1
WPA Pre-shared Key	12345678
Channel-Frequency (AP)	Auto
Channel Spectrum Width	20/40M/80M
Long Range Parameters	Enabled and defaulted to 1000m

Note: A Reset to defaults (performed on the ADMIN page or via the RESET button) will erase all user configurations.

5.0 Quick Configuration

1. Connect an Ethernet cable from the port labelled as IN on the power Injection Module to either a laptop or a PC LAN port.
2. Connect the second Ethernet cable from the OUT port on the Power Injection Module to the NetWave LAN port.
3. Apply 48 VDC to the Power Injection Module with the provided power supply. You should notice the green LED illuminate in the Power Injection Module and the power LED on the NetWave unit.
4. Set the IP address of the laptop being used to configure NetWave to static and the subnet to 192.168.10.x/24 subnet.
5. Point the browser to 192.168.10.101. This is the default address.
For preconfigured kits (NWKX_AP and NWKX_CL) point the Browser to 192.168.10.100 for the Access Point or 192.168.10.101.
6. A login prompt will pop up. Enter:
Username admin
Password admin
7. Select the NETWORK » WIFI tab and set the desired network settings.
Select Apply & Save

Note: *This will be the network address for the NetWave web server. It is not necessary to set to the same subnet as the operating network but it is recommended.*

8. Select the NETWORK -> WIFI tab and set:
 - Country code – Only required if setting up the NW2 (ETSI) model
Note: *It is the user's responsibility to ensure that the correct country is chosen. ComNet accepts no liability for incorrect equipment set up.*
 - Set SSID – if changing from the default setting
 - Channel Spectrum Width – May want to reduce to 20M from the default 20M/40M/80M if the 5GHz spectrum is crowded
 - Wireless Security – if changing from default settings
 - Select Apply Settings
 - Select Save

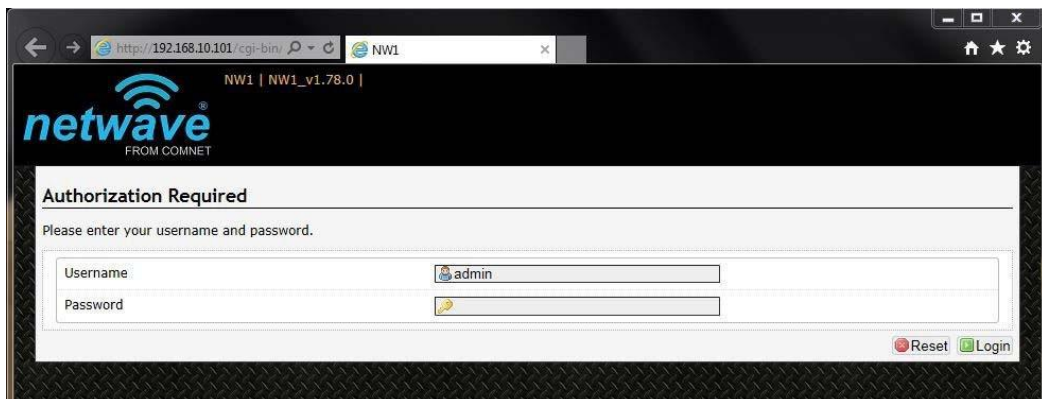
6.0 Detailed Configuration

Getting Started

To access the NetWave configuration interface, perform the following steps:

1. Connect an Ethernet cable from the Data In port on the Midspan Injector or Port 2 on the radio directly to your laptop.
2. If you are using a Midspan Power Injector, Connect the power cable to an outlet and turn on power.
3. Assign the Ethernet adapter on your computer with a static IP address on the 192.168.1.x network, e.g. 192.168.10.10 and with a subnet mask 255.255.255.0.
4. Launch a web browser and enter the default IP address of the device, 192.168.10.101, into the address bar.

The first page that you see is the login page. The words on the top left denote the hardware part number and the firmware build version e.g. NW7 NW7_v1.78.0



The login page is presented upon requesting the Netwave Radio's IP address.

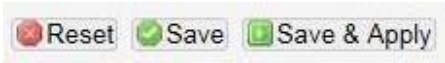
The default authorization details are:

Username: admin

Password: admin

Buttons and Alerts

The buttons are described here.



Reset	Undo the changes.
Save	Saves the changes but does not take effect till settings are applied
Save & Apply	Saves and applies the changes. Please use this button instead of the 'Save' button so that the changes would be applied immediately. It is recommended to click this button before moving to a different page.



Logout	Logs out of the device's web page.
--------	------------------------------------

Note: At the top right corner of the NetWave configuration web page, there may be either of the following texts displayed:

Changes: 0: Means that all changes on the configuration web page have been applied to the Wireless Device.

Unsaved Changes: Shows the number of changes that have not yet been Save & Apply.



Reset Button

 The reset button is a physical button attached to the underside of the radio.

Please refer to Section "Reset Button."

Indicating LEDs

The light emitting diodes (LEDs) on the board are described in Section "Indicator LEDs".

7.0StatusTab

After login, when you click on the Status top-level tab, you can see the second-level tabs of Overview, Routes, System Log, Kernel Log, and Real-time Graphs. This is shown in Figure 2.

Figure 2: The Status Tab.

Overview

The Status » Overview page is divided into the sections Wireless Status, Associated Stations, System, Memory, Network, and DHCP Leases.

Uptime: Displays the duration of time since the NetWave device was turned on or rebooted.



Figure 3: The Status » Overview page.

The Wireless section in the Status » Overview page shows a summary of the wireless parameters. The following describes the parameters when the device works.



Figure 4: A summary in the Wireless section for a device operating as an 802.11 access point.

SSID	Displays the name of the wireless network that this access point is offering, the Service Set Identifier (SSID).
Mode	This is 'Master' if the device works
Channel	Shows the channel number and frequency that this AP is using.
Bitrate	This is the maximum bitrate supported by the radio in the current configuration.
BSSID	This is the MAC address of the AP's radio.
Encryption	Displays the wireless encryption used.

Associated Stations

This section shows the connected devices, if the Radio works.

MAC Address	Network	Signal	Noise	RSSI	TxCCQ	Rx Rate	Tx Rate	HT Mode	Up Time
00:22:38:00:D3:C4	WDS_Station1	-43 dBm	-95 dBm	52(49,43,0)	100%	216 Mbps	300 Mbps	HT40	1 days 23 hours 4 mins 49 s

Figure 6: List of Associated Stations.

If there are no associated Clients, the text “No information available” is displayed. The parameters shown are as follows:

MAC-Address	Displays the MAC address of the station's radio.
Network	States the name of the wireless network.
Signal	Displays the received signal strength from the Client e.g. -26 dBm.
Noise	Displays the received noise power at the AP.
RSSI/Chains	Shows the received signal strengths from the station on each antenna e.g. -42, -26 dBm. The value of -95 dBm is taken to mean “no antenna” if the radio has only 2 antennas. Values inside of the parenthesis show the vertical and horizontal polarities. large difference can indicate a Line of Sight or Noise issue.
TX-CCQ	Indicates the wireless connection quality.
TX Rate	Shows the transmit bit rate from the AP towards this Client.
RX Rate	Shows the receive bit rate at the AP from this Client.
HT Mode	Displays Channel Spectrum Width
Up Time	Display time since last reboot

System

This section shows the Netwave Product name, Firmware Version, Kernel Version, and Local Time.

System	
Router Name	NW1Gen3
Firmware Version	v1.3.1
Kernel Version	2.6.31
Local Time	Thu Jan 1 00:29:14 1970
Uptime	0h 29m 15s

Figure 7: System parameters.

Memory

Here, the Total Available and Free memory are shown.

Memory	
Total Available	81146 KB / 112700 KB (86%)
Free	73024 KB / 112700 KB (64%)

Figure 8: Total Available and Free Memory.

Network

This section displays the status of the LAN and WAN networks.

Network	
IPv4 WAN Status	 Not connected
Active Connections	15 / 34364 (0%)

Figure 10: Network summary.

Status Shows summaries of the interfaces for the LAN and WAN zones. This may include uptime, MAC address, protocol, bytes and packets received by the device, bytes and packets transmitted by the device, and its IPv4 address.

DHCP Leases

This section shows a table of MAC and IP addresses of connected devices with static DHCP leases. They are specified in the Network » Interfaces » LAN » Static Leases section of the device's configuration web page.

DHCP Leases			
Hostname	IPv4 Address	MAC Address	Leasetime remaining
There are no active leases.			

Figure 11: Currently active static DHCP leases.

Routes

When you click on the Status » Routes tab, you would see the page that shows the routing rules that are currently active on the device.

ARP		
IPv4-Address	MAC-Address	Interface
192.168.10.155	3c:97:0e:9a:a7:d2	br-lan

Active IPv4-Routes			
Network	Target	IPv4-Gateway	Metric
lan	192.168.10.0/24	0.0.0.0	0

Figure 12: The Status » Routes page.

- ARP
- This address resolution protocol (ARP) table shows the IP address and corresponding MAC address of each device on the network.
- Active IPv4-Routes
- This table shows the IPv4 gateway and network ID (Target) for each subnet.

System Log

The status page shows system state changes and warning messages.

Status	Network	System	Log
Overview	Routes	System Log	Kernel Log

System Log

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Jan 1 00:01:13 [W]Den3 user.warn kernel: Adding WDS entry for 18:1b1:69:74:67:10, through nl=00:22:3b:0d:d1:72

Figure 13: The Status » Routes page.

Kernel Log

This page shows the kernel debugging messages. This kernel log can also be obtained by typing “dmesg” in a serial console such as Tera Term if a suitable serial connector is used.

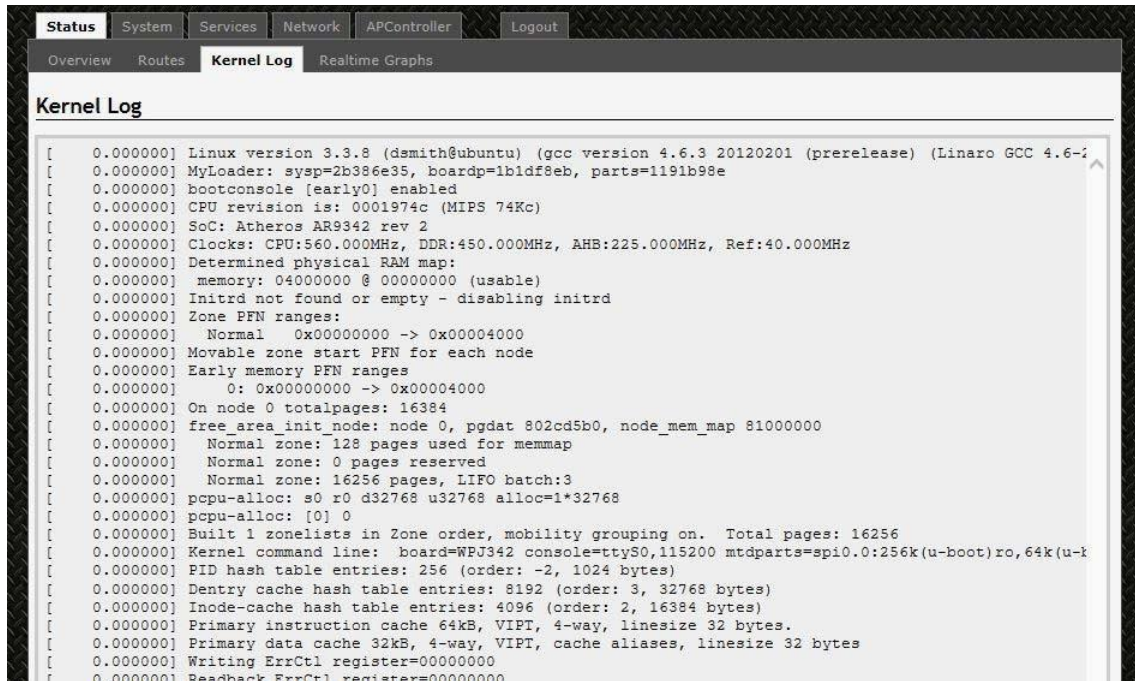


Figure 14: The Status » Kernel Log page.

Real-time Graphs

Under the tab for Real-time Graphs, there are four tabs titled Load, Traffic, Wireless, and Connection.

Load

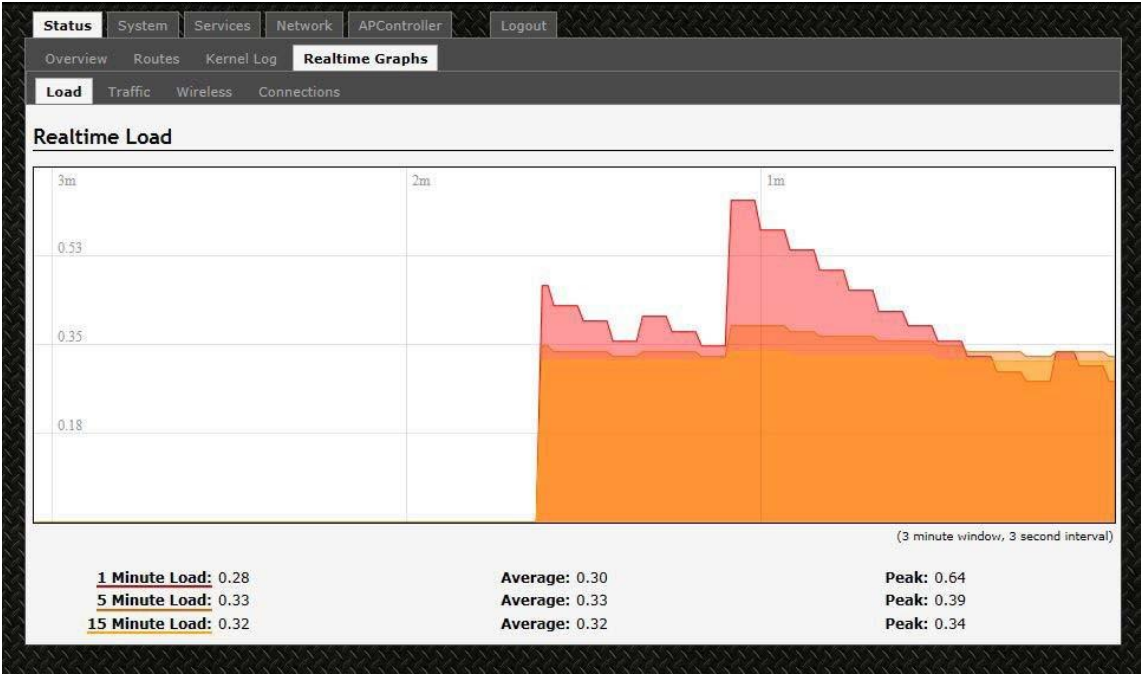


Figure 15: The graph for Real-time Load.

Traffic

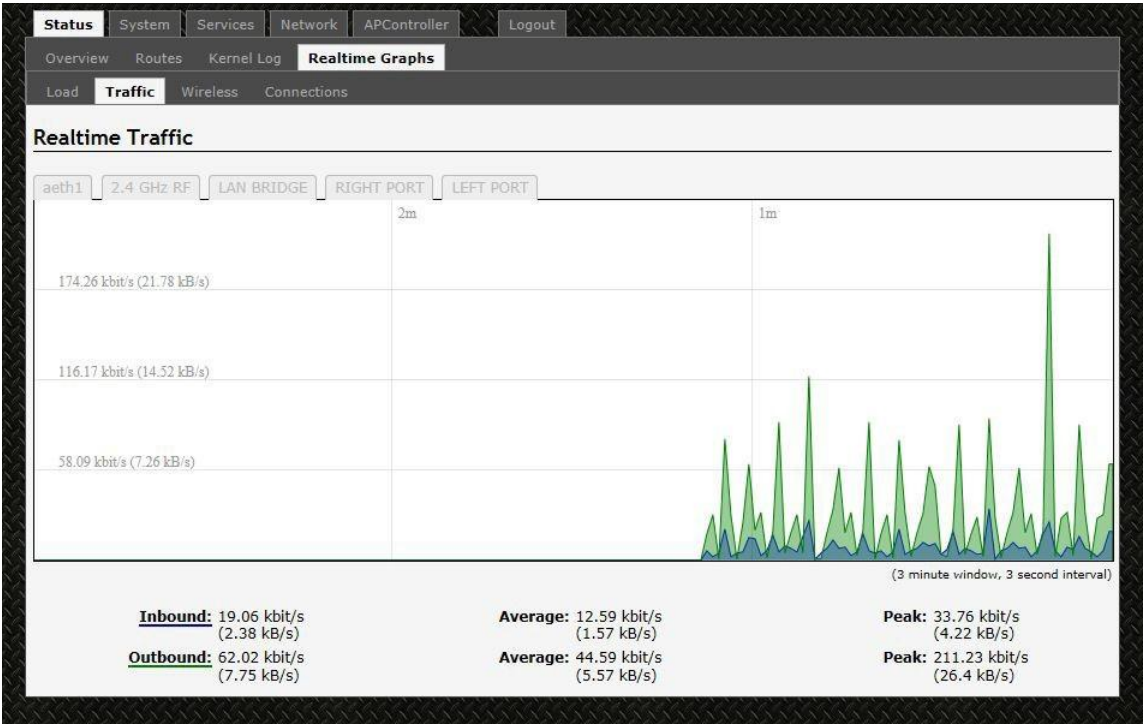


Figure 16: The graph for Real-time Traffic.

Wireless

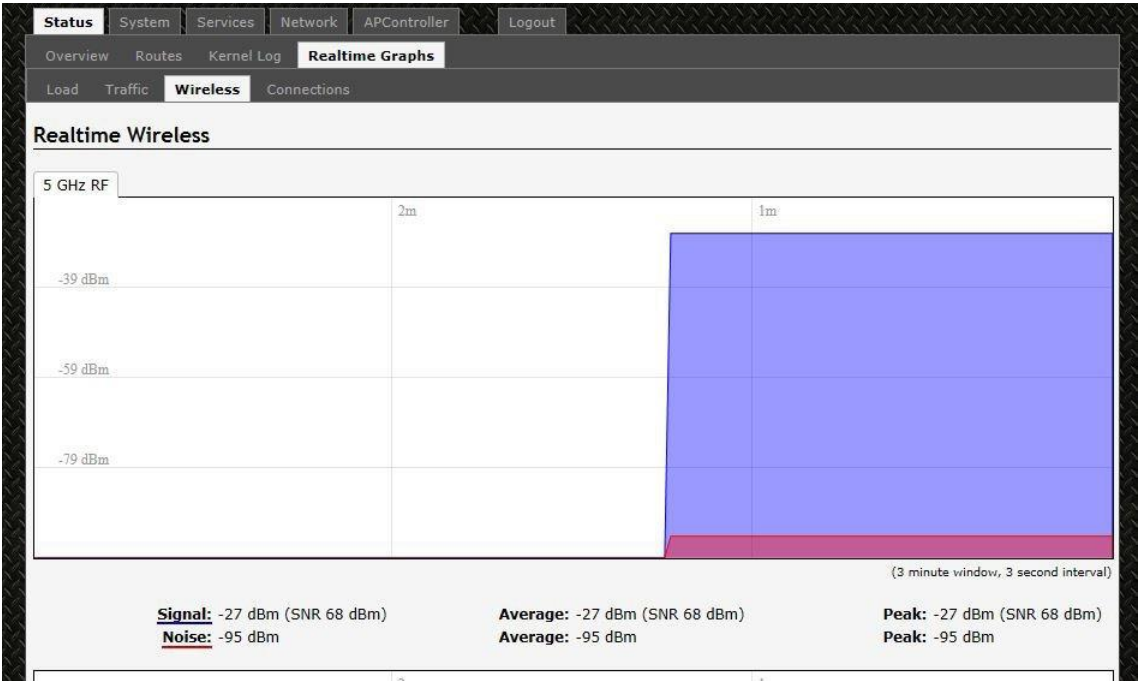


Figure 17: The graph for Real-time Wireless.

Connection

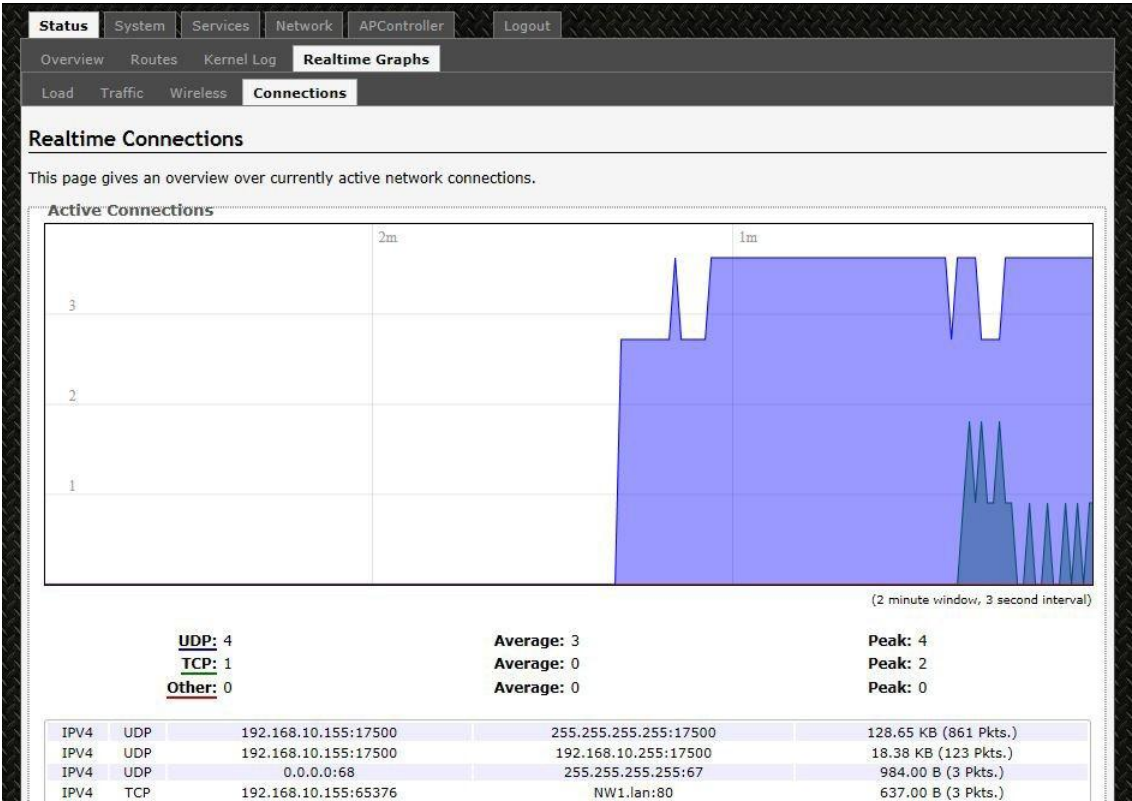


Figure 18: The graph for Real-time Connections.

8.0SystemTab

Within the System >>System page, you can configure the device parameters such as the hostname and time zone.

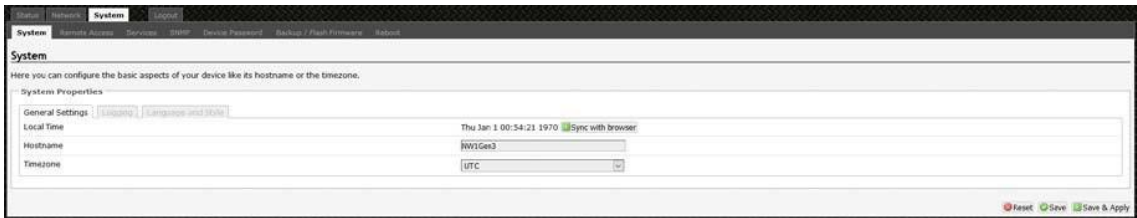


Figure 19:The Systemtop-leveltab.

System Properties

Within the section on System Properties, there are tabs corresponding to General Settings, Logging, and Language and Style.

General Settings

Local Time	Displays the local time according to the time zone.
Hostname	Configures the name of the device.
Time Zone	Sets the time zone.

Logging

System Properties

General Settings

Logging

Language and Style

System log buffer size	16
	kiB
External system log server	0.0.0.0
External system log server port	514
Log output level	Debug
Cron Log Level	Normal

Figure 20: Changing the system properties for Logging.

Logging Specifies parameters used for the system log, such as System log buffer size, External system log server, External system log server port, Log output level, and Cron Log Level.

Language and Style

System Properties

General Settings

Logging

Language and Style

Language	English
Design	OpenWrt

Figure 21:Modifyingthe Language and Style.

Remote Access

Within the System » Remote Access Page, you can configure SSH Network Shell Access.

SSH

SSH

Dropbear offers SSH network shell access and an integrated SCP server.

Interface

☐ lan:

☐ wan: (no interfaces attached)

☒ unspecified

☒ Listen only on the given interface or, if unspecified, on all

Port

☒ Specifies the listening port of this Dropbear instance

Password authentication

☒ ☒ Allow SSH password authentication

Allow root logins with password

☒ ☒ Allow the root user to login with password

Gateway ports

☐ ☒ Allow remote hosts to connect to local SSH forwarded ports

Figure 22: SSH settings in the System » Administration page.

SSH	Allows you to access the device's Linux shell and file system using the Secure Shell protocol. For example, the programs PuTTY and WinSCP can be used.
Interface	Lets the device listen on a given interface or all interfaces.
Port	Specifies the listening port, the default being 22.
Password authentication	Allows SSH password authentication.
Allow root logins with password	This is enabled by default.
Gateway ports	Allow remote hosts to connect to local SSH forwarded ports.

Services

In the System» Services page, you can configure the Ping Watchdog and the Auto Reboot.

Ping Watchdog

Ping Watchdog

Enable Ping Watchdog

☐

IP Address to Ping

192.168.10.1

Ping Interval

5

Startup Delay

60

Failure Count to Reboot

5

Figure 23: Ping Watchdog settings in the System » Services page.

Ping Watchdog	Configures the device to ping to a remote IP address and reboot if the connection is lost. It is disabled by default.
IP Address to Ping	Sets the remote IP address to ping e.g. 192.168.10.10 or 8.8.8.8.
Ping Interval	Specifies the time between successive pings, the default being 5 seconds.
Startup Delay	Sets the time delay after the device finishes rebooting, before running the Ping Watchdog, the default being 60 seconds.
Failure Count to Reboot	Specifies the number of failed pings before the device reboots automatically.

Auto Reboot

Figure 24: Auto Reboot settings in the System » Services page.

Auto Reboot	Allows the device to reboot itself automatically, disabled by default.
Mode	Chooses the Auto Reboot mode by Time or by Number of Hours.
Time	Sets the time of day to reboot if the Mode is by Time.
Number of Hours	Sets the delay as an integer number of hours after each reboot, if the Mode is by Number of Hours.

SNMP

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

In the System » SNMP Page, you can configure SNMP V2c and SNMP V3.

SNMP Information

In the SNMP Information section, the text fields for the SNMP Enterprise ID, Contact, and Location information are shown.

SNMP Configuration

General Settings

SNMP Configuration

General Settings

Trap

Enable SNMP	☒
SNMP V2c Read Password	public
SNMP V2c Write Password	private
SNMP V3 Username	admin
SNMP V3 Auth Algorithm	MD5
SNMP V3 Auth Password	••••••••
SNMP V3 Privacy Algorithm	DES
SNMP V3 Privacy Password	••••••••

Figure 25: General settings for SNMP.

Enable SNMP	Enables SNMP.
SNMP V2c Read Password	Sets the community string for read-only access (to the variables on the SNMP agent) by the network management station (NMS). The NMS is the software which runs on the SNMP manager. (default: public)
SNMP V2c Write Password	Sets the community string for read-write access by the SNMP manager. (default: private) A community string identifies a group of SNMP agents. It is sent in clear text. It should be changed from the default string “public” or “private”. The variables on the SNMP agent can be classified into read-only or read-write variables.
SNMP V3 Username	Sets the username for authentication. (default: admin)
SNMP V3 Auth Algorithm	Shows the authentication algorithm used e.g. MD5.
SNMP V3 Auth Password	Configures the password for user authentication. (default: password)
SNMP V3 Privacy Algorithm	Shows the data encryption algorithm used e.g. DES.

SNMP V3 Privacy Password Sets the password for data encryption. (default: password)

Trap

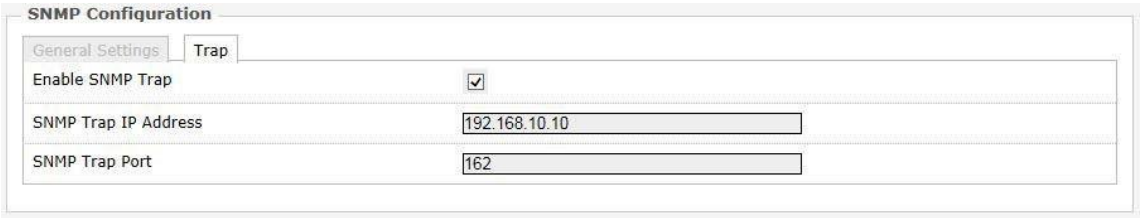
The image shows a web interface for 'SNMP Configuration' with a 'Trap' tab selected. It contains three fields: 'Enable SNMP Trap' with a checked checkbox, 'SNMP Trap IP Address' with the value '192.168.10.10', and 'SNMP Trap Port' with the value '162'.

Figure 26: SNMP trap configuration.

Enable SNMP Trap	Allows the SNMP agent to notify the SNMP manager of events.
SNMP Trap IP Address	Sets the IP address of the SNMP manager which receives the trap messages.
SNMP Trap Port	Sets the port number.

Device Password

Change Administrator Password.

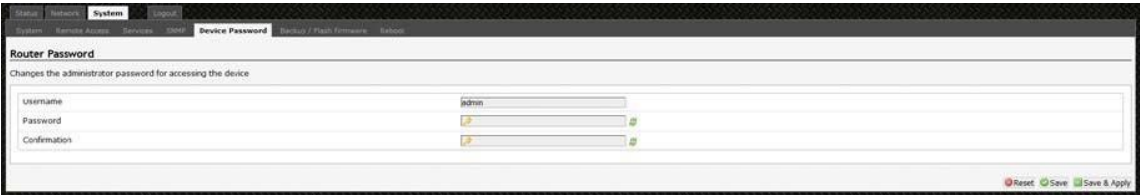
The image shows a 'Router Password' configuration page. It has a title 'Router Password' and a subtitle 'Changes the administrator password for accessing the device'. There are three input fields: 'Username' with the value 'admin', 'Password', and 'Confirmation'. Each password field has a strength indicator icon (a green 'a' in a circle). At the bottom right, there are buttons for 'Reset', 'Save', and 'Save & Apply'.

Figure 27: Signal strength indicator LEDs and their default threshold values in dBm.

Backup/Flash Firmware

The System » Backup/Flash Firmware page lets you perform backup and restore, or flash a new firmware.

Backup/Restore

Download backup Generate archive: Downloads a tar archive of the current configuration files.

Note: The backup archive file should be stored in a safe place because it contains the wireless password in clear text.

Reset to defaults Perform reset: Resets the firmware to its initial state.

Restore backup Upload archive: Lets you upload a previously generated backup archive to restore configuration files.

Flash new firmware

You can upload a new firmware to replace the currently running firmware.

Keep settings Retains the current configuration.

Firmware Shows the current version of the firmware and allows you to upload a new firmware.

Reboot

Perform reboot Reboots the operating system of your device. This is similar to the power-off and power-on cycle. The system configuration remains the same. Any changes that are not applied are lost.

WiFi -Overview

Clicking on the Network » WiFi tab would bring you to the Wireless Overview page. This page shows the radios present on the device. .

The wireless local area networks (WLANs) are displayed under each radio.



Figure 31: The Wireless Overview page showing one radio.

Scan	Shows available access points on specified channels
Add	Allows you to add virtual access points (VAPs) to the radio. By default, there is only one VAP on the radio. Each VAP corresponds to one network.
Enable	Enables the radio.
Disable	Disables the radio.
Edit	Brings you to the configuration page of the network. Clicking this button is equivalent to clicking the corresponding tab above.

Associated Stations

Associated Stations will show a list of devices connected to the Radio.



Figure 32: The Associated Stations are also shown on the Wireless Overview page.

The Various Performance Parameters are displayed.



WiFi – Wireless Network

As mentioned earlier, clicking on the Edit button for a network would bring you to the configuration page. This page contains the sections Device Configuration and Interface Configuration.

The Device Configuration section covers the physical settings of the radio hardware such as channel, transmit power, or antenna selection. These are shared among all defined wireless networks of the radio. Per network settings like encryption or operation mode are grouped in the Interface Configuration.

Device Configuration

The Device Configuration section consists of the section tabs for General Setup and Advanced Settings.

General Setup

Status Shows a summary of the wireless network.

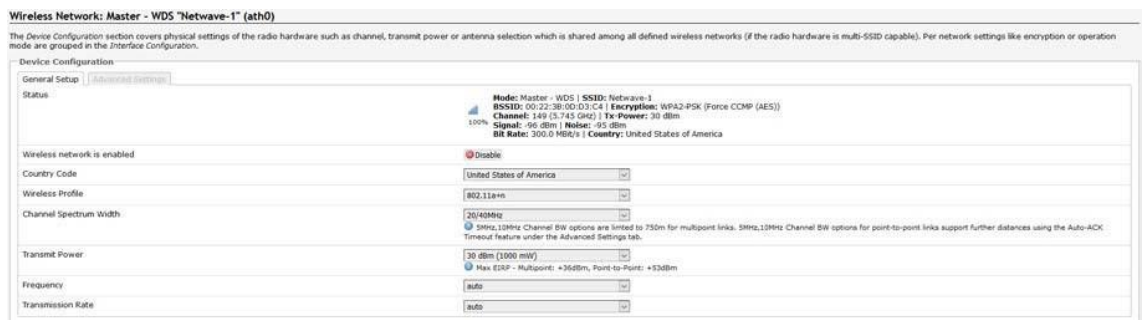


Figure 34: The WiFi Device Configuration section. FCCVersion. European Radiosinclude a Channel Scan List.

WPA or WPA2 with EAP

The Extensible Authentication Protocol (EAP) is encapsulated by the IEEE 802.1X authentication method. IEEE 802.1X is equivalent to EAP over LAN or WLAN. Enterprise networks commonly use this authentication method.

WPA or WPA2 with EAP

Interface Configuration

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Encryption

IEEE802.1X/WPA-EAP

Cipher

CCMP (AES)

Radius-Authentication-Server

Radius-Authentication-Port

Default 1812

Radius-Authentication-Secret

Radius-Accounting-Server

Radius-Accounting-Port

Default 1813

Radius-Accounting-Secret

NAS ID

Figure 39: Encryption options for WPA-EAP or WPA2-EAP in AP mode.

Cipher	Can be set to Auto, CCMP (AES), or TKIP and CCMP (AES).
Radius-Authentication-Server	Specifies the IP address of the RADIUS authentication server. Note: Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.
Radius-Authentication-Port	Sets the port number for the RADIUS authentication server. Normally, the port number is 1812.
Radius-Authentication-Secret	Configures the password for the authentication transaction.
Radius-Accounting-Server	Specifies the IP address of the RADIUS accounting server.
Radius-Accounting-Port	Sets the port number for the RADIUS accounting server. Normally, the port number is 1813.
Radius-Accounting-Secret	Configures the password for the accounting transaction.
NAS ID	Specifies the identity of the network access server (NAS).

WPA or WPA2 with EAP

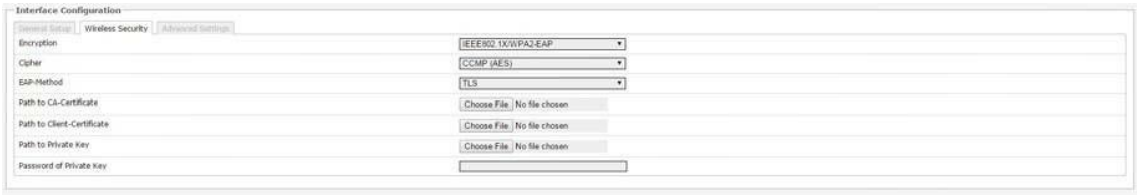


Figure 40: Encryption options for WPA-EAP or WPA2-EAP in Client mode.

Cipher	Only Cipher option is CCMP (AES)
EAP-Method	The authentication protocol can be set to Transport Layer Security (TLS), Tunneled TLS (TTLS), or Protected EAP (PEAP).
Path to CA-Certificate	Selects the file for the CA certificate. Note: The certificate authority (CA) is a trusted third party that issues digital certificates. In a public key infrastructure scheme, a digital certificate certifies the ownership of a public key by the named subject of the certificate.
Path to Client-Certificate	Selects the file for the client certificate.

Options for TLS as the EAP method

Path to Private Key	Selects the file for the private key.
Password of Private Key	Configures the password for the private key.

Options for TTLS or PEAP as the EAP method

Authentication	Selects the authentication method used by the AP, e.g. PAP, CHAP, MSCHAP, or MSCHAPV2.
Identity	Sets the identity used by the supplicant for EAP authentication.
Password	Sets the password used by the supplicant for EAP authentication.

MAC-Filter

This section tab is only available for a device operating as an AP.

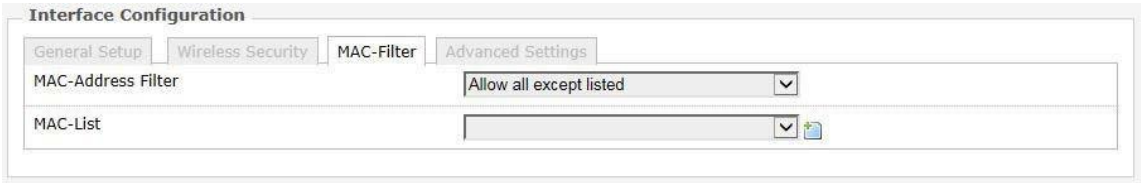


Figure 41:Configuring the MAC-Filter for a Wifi AP.

MAC-Address Filter	Lets you allow only devices with the listed MAC address to associate with this AP, or lets you block devices with the listed MAC address.
MAC-List	Adds the MAC address of the remote device to either block or allow.

Advanced Settings

Figure 42: Advanced Settings for the Wifi Interface.

Separate Clients	Prevents station-to-station communication, unchecked by default. When Station Isolation is disabled, wireless clients can communicate with one another normally by sending traffic through the AP. When Station Isolation is enabled, the AP blocks communication between wireless clients on the same AP.
Maximum Stations	Specifies the maximum number of associated stations, the default being 127.
Limit RSSI	Sets the minimum received signal strength indicator for a station to be associated. The default value of 0 means that the AP would allow a station to associate independent of its RSSI.

VLAN

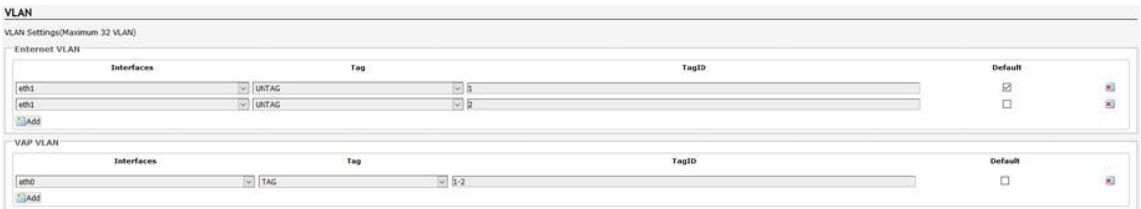


Figure 43: Advanced Settings for the Wifi Interface.

VLAN Settings page allows you to assign specific VLANs to an interface. VAP VLAN is the Virtual AP VLAN Connection over the wireless port.

9.0 GPL (General Public License) Statement

You may have received from ComNet products that contained – in part – free software (software licensed in a way that ensures your freedom to run, copy, distribute, study, change and improve the software). Such products include NetWave series of products.

As part of these products, ComNet may have distributed to you hardware and/or software that contained a version of free software programs developed by the Free Software Foundation, a separate not-for-profit organization without any affiliation to ComNet.

See <http://www.gnu.org/philosophy/free-sw.html> for more details. If ComNet distributed any portions of these free software programs to you, you were granted a license to that software under the terms of either the GNU General Public License or GNU Lesser General Public License “License”, copies of which are available from <http://www.gnu.org/licenses/licenses.html>. The Licenses allow you to freely copy, modify and redistribute that software without any other statement or documentation from us.

ComNet will provide to anyone who contacts us at the contact provided below, for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the free software programs used in the version of the programs that we distribute to you. The cost will be free if the delivery medium of the machine-readable copy is through the Internet.

Contact information:

Email: techsupport@comnet.net

Tel: 203-796-5300

Address: 3 Corporate Drive, Danbury, CT 06810 USA

We will reply within 7 working days once the request has been made through email or telephone.

ComNet Customer Service

Customer Care is ComNet Technology’s global service center, where our professional staff is ready to answer your questions at any time.

Email ComNet Global Service Center: customercare@comnet.net

Contact Information

ComNet – www.comnet.net

North America	ComNet Corporate Headquarters and Customer Support Center	Tel: +1-203-796-5300
		Tel: +1-888-6789427
		Email: info@comnet.net
EMEA, PACRIM, South America	ComNet Europe Ltd, Leeds	Tel: +44 (0)113 307 6400
		Tel: +44 (0)113 307 6409
		Email: info-europe@comnet.net



3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET

FCC Statement

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

ISED RSS Warning:

This device complies with Innovation, Science and Economic Development Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISED RF exposure statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Le rayonnement de la classe B respecte ISED fixaient un environnement non contrôlés. Installation et mise en œuvre de ce matériel devrait avec échangeur distance minimale entre 20 cm ton corps. Lanceurs ou ne peuvent pas coexister cette antenne ou capteurs avec d'autres.

Note : This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.